WES Pro User Guide

Release 1.0

Michael Kline <support@fortrobotics.com>

Aug 18, 2025

TABLE OF CONTENTS

WES PRO USER GUIDE

This book describes the FORT Pro series devices.

CHAPTER

ONE

INTRODUCTION

This document shows how to integrate the FORT Wireless E-Stop Pro (WES Pro) device with your smart machines to enable secure transmission of wireless safety and control commands. FORT helps protect people and organizations from injury, damage, and downtime with trusted control & communication for any machine. With built in functional safety and security, FORT's Pro Series delivers machine control and communication you can trust.

The WES Pro is part of the Pro Series of devices, which includes:

- **Wireless E-Stop Pro (WES Pro)** A handheld device that sends a wireless E-Stop command to connected machines[1] with the push of a button.
- **Endpoint Controller (EPC) —** A mountable sender and receiver that can execute trusted commands over Bluetooth low energy, Wi-Fi, Ethernet, and ISM Radio. It can be used as a sender, to send safety signals to other FORT devices, such as NSC Pros or other Endpoint Controllers, or as a receiver, wired into a machine for control and safety functions sent by another FORT device, such as an Endpoint Controller or a Safe Remote Control Pro with which it is paired.
- **Safe Remote Control Pro (SRC Pro) —** Used as a sender to wirelessly connect to an Endpoint Controller, it provides both wireless E-Stop and remote operator control of a machine at a safe distance.
- **Nano Safety Controller Pro (NSC Pro) —** An embedded board with a small form factor that allows OEM developers to build emergency stop (E-Stop) functionality directly into their machines without requiring bolt-on hardware. The NSC Pro controls a machine (known as the EUC, or equipment under control) by receiving safety signals from an Endpoint Controller or Safe Remote Control Pro with which it is paired.
- **FORT Manager —** Provides device registration, configuration, management and updates, and management of users through a web-based application and a desktop application. Access the FORT Manager Web App to use the UI to build a configuration. You can download the desktop application from the FORT Manager web app. It provides additional functionality not found in the web app.

This guide is intended for integrators who want to implement safety solutions in their machines as well as operators of those machines.

Key Features

The WES Pro is a sender that pairs with an EPC receiver[2] to support integration into a wide variety of simple, semi-autonomous, and very intelligent systems.

Some key features of the WES Pro are:

[1] For the initial release, a WES Pro can pair with one receiver only. Consult the Release notes for information specific to the version of the product that you are using.

[2] For this release, a WES Pro can pair with one receiver EPC only. Consult the Release notes for information about the type and number of devices a WES Pro can pair with that is pecific to the version of the product that you are using.

- 12 hour battery life. The device charges through a charging dock equipped with a with USB-C interface to a power supply.
- Lightweight handheld device that fits in your palm; 43 mm x 60 mm x 180 mm (1.69” x 2.36” x 7.09”)
- Wireless interface that supports Long Range Bluetooth Low Energy (LRBLE) with a range of 100–300 m LOS.
- CANopen and J1939 interface[3] for data and status communications.
- Pairs with an EPC receiver to send one, dual-channel safety command[Page 2, 2] . The dual safety processors are the core of a redundant, one out of two (1oo2) safety architecture.
- Operates in temperatures from -20 °C to 60 °C.
- IEC 61508 certified (pending).

See *Technical Specifications* for detailed specifications for the WES Pro.

Overview

The primary function of the system, comprising a transmitter and receiver(s) (in this case a WES Pro transmitter and an EPC receiver) is the ability to wirelessly send a safety signal from the transmitter to the receiver that is attached to the equipment (henceforth known as the EUC, or equipment under control), causing the the EUC to move from the normal state to the safe state.

The **safe state** causes the equipment under control (EUC) to cease whatever function it is performing. Depending on the equipment and how you wired and configured it, this could mean shutting down the machine entirely, slowing it down, turning off a specific function such as a robotic arm, or something else entirely. Depending on the implementation, any of the following situations trigger the safe state:

- An equipment operator perceives that the EUC has encountered a major problem that requires it to be stopped or slowed down immediately and presses a button to send an E-Stop signal to do so.
- The system detects an automatic diagnostic fault and initiates the safe state.

The **normal state** means that an E-Stop command has not been requested, no diagnostic faults are detected, and the EUC is powered.

[3] For this release, CAN is not supported. Consult the Release notes for information specific to the version of the device that you are using.

There are various ways to configure the system, using FORT Manager, depending on your specific situation, but at a basic level, every configuration has:

- A network that allows devices to communicate.
- A FORT Pro receiver embedded in or attached to each EUC (in this case, an EPC attached to the equipment).
- A sender (in this case, a handheld WES Pro) that communicates wirelessly to send safety signals to the FORT device(s) attached to the EUCs.

The following figure illustrates a basic configuration:

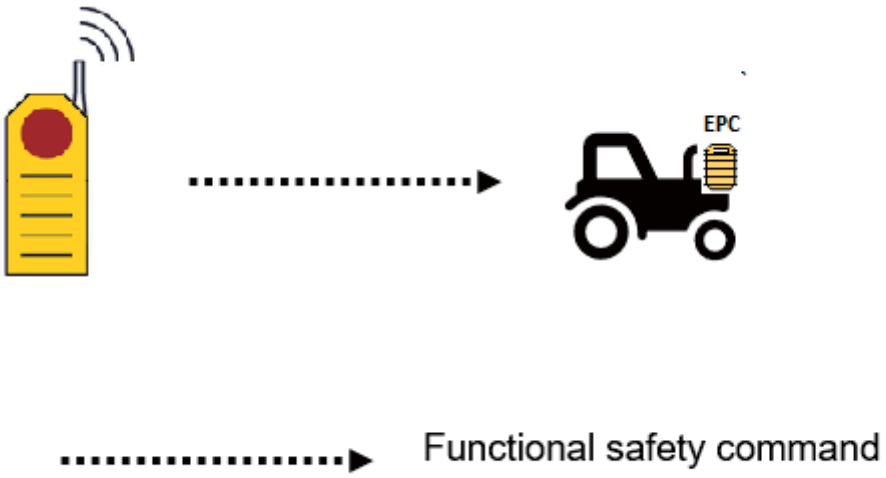

Fig 1.1: Basic Configuration

Showing just a one-to-one configuration looks pretty lame. Maybe genericize this whole section and show a figure with multiple devices?

Implementation Process

The following bullets outline the process for getting your Pro Series devices up and running. Although we show Plan as the first step, this manual assumes that you have already determined how many devices you need and have purchased them.

- **Plan —** Determine the type of configuration to build. *Configurations and Use Cases (WES Pro)* provides an overview to the types of configurations that we support and the use case for each one. In addition, be certain to involve a safety expert in the planning process to develop a safety plan for integrating the FORT Pro Series devices with your equipment.
- **Wire —** Wire the outputs for your receiver(s) (for example, Wiring EPC Receivers in the Pro Series documentation).
  - Your sender is a WES Pro so no wiring is necessary because the E-Stop is built into it.
  - Wire the receiver output(s) (EPC) to the EUC (Wiring EPC Receivers in the Pro Series documentation).
- **Configure —** Use FORT Manager to build a logical configuration (*Building a Configuration*):
  - Log into FORT Manager and register your devices; if you don't have access to FORT Manager, email us at *support@fortrobotics.com* to get started.

  - Add them to a configuration.
  - Set device and network parameters, including communication channels, timeout value, and types of inputs.
- **Load —** Load the configuration onto each device.
- **Test —** Verify that the system performs as expected before deploying it. For example, pressing an E-Stop button stops the EUC, walking in front of a light curtain slows or stops the EUC, and so on. Be certain that a safety expert verifies that the system is operating in accordance with your safety plan.

Warning

Safe operation of the system requires that you thoroughly test the system before putting it into a production environment. Testing includes training your personnel on both the manual functions (pressing an E-Stop button, using an SRC Pro to maneuver an EUC, etc.) and automatic functions of the system (solid state devices triggering safety, exceeding the timeout value, loss of radio signal, etc.).

Getting Started

This section is named for the *Getting Started Guide* on the FORT Website. The starting point for that guide is to accept the invite to FORT Manager and register your devices. Is this where we want to start?

If you haven't done so already, follow the instructions in the Getting Started Guide to set up a FORT Manager account and register your devices. FORT Manager enables you to build secure and functionally safe device configurations. However, FORT Manager also allows you (or someone in your organization) to:

- View current configurations and device utilization.
- Set up your organization, manage user accounts, and assign roles.
- View and submit support tickets.
- Update firmware as necessary.

Note

If you are having any problems with the FORT Manager App (accessible in a Web browser or available as a downloadable desktop application) such as launching or logging in, or you don't have the serial number for your devices, submit a request on the Support Portal to get help. Click **Sign up** to create a Zendesk account if you don't already have one.

Next Steps

Depending on your role, go to:

- *Using a WES Pro* to familiarize yourself with your WES Pro device.
- *Configurations and Use Cases (WES Pro)* for instructions on building a device configuration.
- Wiring EPC Receivers in the Pro Series documentation for hardware wiring instructions.

CHAPTER

TWO

CONFIGURATIONS AND USE CASES (WES PRO)

After you register your FORT Pro Series devices, you can add them to a configuration in FORT Manager, which is available as both a web-based and a desktop application.

A configuration allows you to[1] :

- Add devices to a network enabling them to communicate with each other.
- Configure device settings.
- Select the method for device communication.
- Designate the type of sender for the configuration (EPC, WES Pro, SRC Pro).
- Designate the type of receivers for the configuration (EPC, NSC Pro).
- Configure the inputs on the sender.

The following table shows the various configurations that you can build with a WES Pro sender:

Table 2.1: Configurations

Configuration Type	Sender:Receivers[2]	Definition
One-to-One (1:1)	WES Pro : EPC;	One sender connected to one receiver.
Two-to-One (2:1)	SRC Pro & WES Pro : 1 EPC;	Two senders, each able to send a safety signal to the connected receiver.

You use FORT Manager to build these configurations and your laptop to apply the configurations. You can find instructions for building any type of configuration in *Building a Configuration* and instructions for loading configurations to your devices in *Loading a Configuration onto a WES Pro*.

One-to-One Configuration

In a One-to-One (1:1) configuration, you configure a single WES Pro sender connected to a single EPC receiver.

The following table shows details about a One-to-One configuration

Table 2.3: One-to-One Configurations

[1] Not all of these functions are available for every type of configuration. For example, you don't configure inputs on an SRC Pro or WES Pro, the method of communication may be predetermined by the device model so it can't be set in FORT Manager, etc.

[2] Consult the Release notes for information specific to the version of the product that you are using regarding the type and number of devices that can be paired together.

Sender : Receiver	Inputs	Communication
WES Pro : EPC	One safety rated input	LRBLE

The following figure shows a One-to-One configurations:

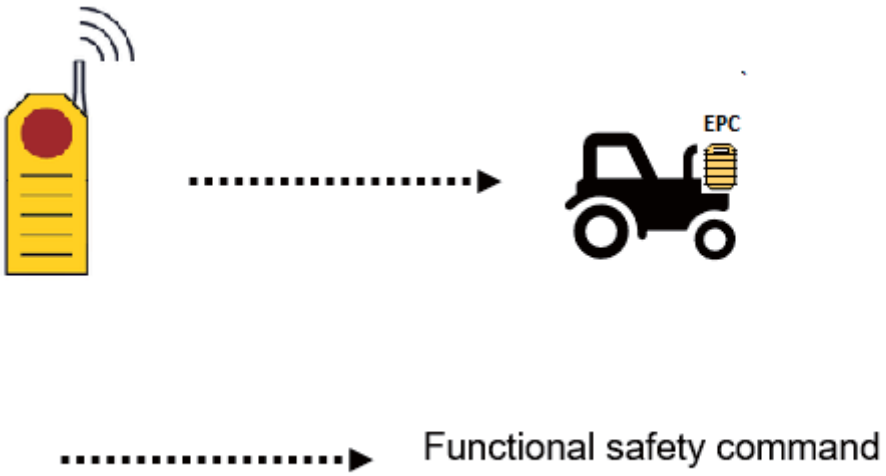

Fig 2.1: One WES Pro to EPC Configuration

Two-to-One Configuration

A Two-to-One (2:1) configuration has two senders and one receiver, which allows either of two people to send an E-Stop signal to the receiver and the EUC. This section describes a configuration with SRC Pro and WES Pro senders and one EPC receiver.

For example, the equipment operator controls the machine with an SRC Pro and can push the E-Stop button at any time to resolve a safety issue. At the same time, another person can observe the operation from a different vantage point and press the E-Stop on the WES Pro or the EPC if they see a safety issue.

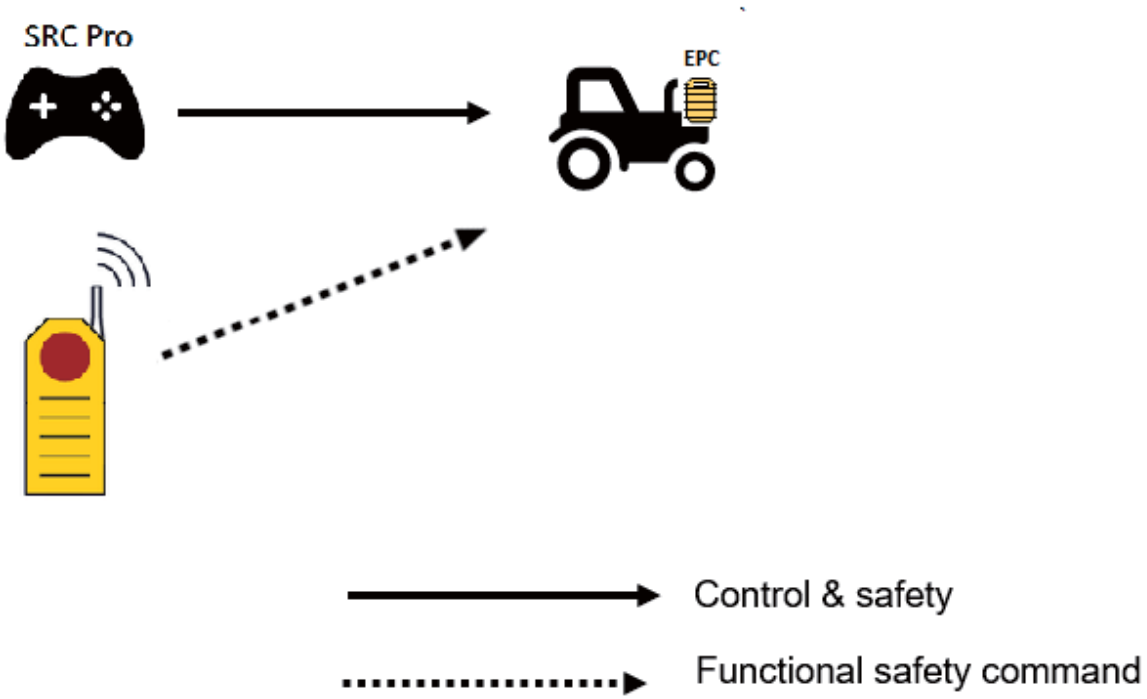

Fig 2.2: SRC Pro & WES Pro to EPC Configuration

The following table shows details about a Safe Remote Control Pro configuration:

Table 2.5: Safe Remote Control Configuration

Sender	Inputs	Receivers	Communication
SRC Pro & WES Pro	Integrated E-Stop switch	One EPC	Long Range Bluetooth (LRBLE)

Building a Configuration

Use the FORT Manager Web App or Desktop App to build a configuration. These instructions are applicable to all types of configurations.

Before you Begin

Make sure that:

- You've created a FORT Manager account and added your devices to FORT Manager.
- You know what kind of configuration you plan to build (refer to the *Configurations table*).
- You know the details of your IP network:
  - If using Ethernet, the gateway address, range of available IP addresses, netmask, and optional DNS server.
  - If using Wi-Fi, network name and password, gateway address, range of available IP addresses, netmask, and optional DNS server.

- If using CAN, which protocol, CANopen, or J1939. Both are disabled by default.

To Create a Configuration and Add Devices

(Requires the FORT Manager ConfigManager or Admin role.)

> **Note**
>
> The following instructions are complete as far as creating a configuration and adding devices to it. The instructions for configuring settings will get you started but are not comprehensive. However, the FORT Manager interface is intelligent and provides prompts and warnings to guide you through setting parameters, and adjusts the available options based on choices you make. For example, if you select Wi-Fi for communication, you are prompted for the name and password of the network, if you select Ethernet, you are prompted for the IP address, etc.

1. Navigate to the FORT Manager Web App and enter your credentials when prompted.
2. Click **Configurations** in the left navigation pane.
3. Click **New Setup**.
4. On the **Setup Details** page, select **use WESP as my controller**

a. If you are using a single sender, click **Continue** to accept the default of no secondary sender.

b. If you want to use have a WES Pro with an SRC Pro, select select **Yes** for SRCP as a secondary controller.

5. In **Setup Name**, type a name to identify your configuration and click **Continue**.
6. On the **Select Sender** page, select a device to use from the list to use as a sender and click **Continue**.
7. Optionally, select the second controller (if you chose this configuration in Step 4) and click **Continue**.
8. On the **Select Receiver(s)** page, select receivers from the list and click **Review Setup**.

FORT Manager displays the sender(s) and receiver(s) in the configuration and displays the following message to alert you if settings are incomplete:

```
This configuration is incomplete. Go to the settings page to add missing info.
```

Go to the next procedure to configure settings.

To Configure Settings

FORT Manager displays the **Warning** symbol next to the Settings menu, as well as next to the General or Devices tabs on the Settings menu if any settings need to be configured.

> **Note**
>
> If you need help with any particular setting, click the info icon next to it to see more information.

1. Click **Settings** to configure settings for the new configuration.
2. Click **General** to configure settings that apply to all devices in the configuration.

> **Note**
>
> For all configurations, you must specify a safety timeout.

3. Click **Save** to save the general settings.

4. Click **Devices** and select a device from the drop-down list to configure settings specific to each device.

   FORT Manager displays the Warning symbol next to any device that requires you to configure settings.

5. Click **Save** when you've completed configuration of all devices.

Configuration Parameters

The FORT Manager interface is intelligent:

- It notifies you that the configuration is incomplete and displays the Warning symbol next to tabs and devices that contain settings that must be set.
- It highlights fields that are required.
- It highlights additional fields based on settings you choose; for example, if you select Wi-Fi for communication, you are prompted to enter a network name and password, if you select Ethernet, you are prompted for an IP address.
- Every setting has an information icon that you can hover over to get more information.

The following table lists and describes all the configuration parameters for a WES Pro in FORT Manager:

Table 2.7: Safe Remote Control Configuration

Type	Parameter	Required	Description
General	Output to Control	Required	Select whether to control
General	Safety Timeout	Required	During normal operation, a receiver EPC expects to receive
General	CAN Mode	Optional	Select
General	CAN Bitrate	If CAN Mode is CANOpen	Optimal
Device (receiver)	CAN Node ID	If CAN is enabled	ID

CHAPTER

THREE

LOADING A CONFIGURATION ONTO A WES PRO

After you build a configuration, you need to load it onto your devices in one of the following ways:

- By using the FORT Manager Desktop application (*Using the Desktop App to Load a Configuration onto a WES Pro*).
- By using the CLI tool (*Using the Desktop App to Load a Configuration onto a WES Pro*).

Using the Desktop App to Load a Configuration onto a WES Pro

Note that this procedure requires the FORT Manager *Desktop* app, not the *Web* app; if you don't already have it, you can download the Desktop app, Windows or Linux version, from the Web app or directly from GitHub.

To Load a WES Pro Configuration using FORT Manager Desktop App

Required Items:

- A configuration that you built in FORT Manager.
- Windows or Linux computer running with Ethernet networking capability (required for using the FORT Manager Desktop app).
- The WES Pro docking station.
- FORT Manager Desktop app (find latest version in FORT Manager or at GitHub).
- The WES Pro is in a safe state to be configured.

1. Launch the FORT Manager Desktop app on your computer.
2. Connect the USB cable to a port on your computer.
3. Turn the docking station over and insert the USB-C connector on the cable into the port on the underside of the docking station:

Fig 3.1: Docking Station Underside

4. Push the WES Pro into the docking station until it clicks in place. The application displays a message that it has detected a device for tethering.

> **Note**
>
> If the device is not automatically detected, click **Tether a Device** in the left pane, select **WESP** as the type of device, enter the port in **Path** (generally *COM3*), and click **Connect**.

5. Select the device and click **Tether**. The application displays information about the device including the name of the configuration to which the device belongs.
6. Click **Update** next to the configuration name to upload the configuration to the device.

The application shows that the configuration has been uploaded and automatically untethers the device. You can unplug the device from the computer unless you have a firmware update to apply as well.

To Download Configuration for Offline Loading

One of the advantages of the desktop app is that you can use it without an internet connection. If you plan to load configurations or make firmware updates when the internet is not available, you can download the firmware and configurations when connected to the internet and store them in the app for later retrieval.

1. Launch the FORT Manager Desktop app on your computer.
2. Click **Configurations**.
3. Select the configuration to download.
4. Click **Download Configuration**.

The Download Status changes to *Downloaded*.

Repeat for any other configurations that you plan to upload when offline.

> **Note**
>
> Downloaded files are stored in the application, not in the computer's file system, which means you access them through the Desktop app, *not* in the downloads file on your computer.

Using the CLI Tool to Load a Configuration onto a WES Pro

When using the FORT CLI tool, you don't need to download the configuration. The CLI tool connects to FORT Manager and locates the proper configuration based on the device serial number that you enter.

To Load a WES Pro Configuration with the CLI Tool

Required Items:

- A configuration that you built in FORT Manager.
- Linux computer running Ubuntu with Ethernet networking capability.
- The WES Pro docking station.
- FORT CLI Configuration Tool, `fort_cli_cfg` (find latest version in FORT Manager). Download a PDF Copy of the Pro Series User Guide for other requirements of setting up the CLI tool.
- The WES Pro is in a safe state to be configured.
- You have on hand the device serial number (found on the plate on the device or in FORT Manager).

1. Turn on the WES Pro, place it in the docking station, and connect the docking station via USB to the computer.
2. In a Linux environment, open a Terminal window and navigate to the folder containing the FORT CLI configuration tool.
3. Run a command similar to the following to launch the configuration tool for the WES Pro (your `/dev/tty` port could be different):

   ```
   $ fort_cli_cfg -w -n /dev/ttyACM0
   ```

   The parameters you specify for the CLI tool are as follows:

   `-w (--web)`
   Specifies to upload a single configuration from FORT Manager.

   `-n (--nxp) /dev/ttyACM0`
   Specifies a WES Pro device and identifies the USB port in use; your port could be different.

   Note that you need execute permission to `/dev/ttyACM0`, or whichever virtual port you are using for the WES Pro. If you receive a permission error, complete the next two sub steps, otherwise continue to Step 4:

   a. Run the following command to add yourself to the *dialout group*:

      ```
      sudo -a -G dialout $USER
      ```

   b. After running the command, log out of the Linux session, then log back in and rerun the configuration tool.

   The CLI tool returns a code. The browser opens a window that asks you to confirm that the displayed code matches that in the CLI tool.

4. Press **Enter** to confirm that the codes match.

5. If you aren't already authenticated, enter your FORT Manager username and password to authenticate to FORT Manager.
6. Return to the CLI tool where you are prompted to enter the device serial number: `Enter device serial number:`
7. Type the serial number (found on the WES Pro device and also in FORT Manager on the Devices page) and press **Enter**.
8. Press **Enter** to load the configuration to the device. The tool finishes with the WES Pro by writing all the relevant configuration parameters.
9. Reboot the WES Pro.

CHAPTER

FOUR

USING A WES PRO

This chapter describes the features of the WES Pro and explains how to connect a WES Pro to a receiver.

Charging the WES Pro

This section could also be an insert that comes in the box with the WES Pro, basically a getting started guide. Or, have a Zendesk article with the same?

The WES Pro is shipped with a docking station and a power supply and cable for charging the device.

The cable and power supply in the figure are a placeholder; need the actual power supply. Also, do we need to warn them about using a power supply that is more or less than what we specify and ship it with?

Fig 4.1: Docking Station Charger & WES Pro

To Charge the Device

> **Warning**
>
> Always charge the device where the dock is not exposed to dust or moisture. If the dock is wet, towel it off before charging the device.

Caution

To prevent unintended machine startup, press the E-Stop button on the WES Pro before inserting it into the dock. If you power off the WES Pro to disconnect from a receiver, when you place it in the dock for charging, it automatically powers back on and reconnects to the receiver, potentially triggering the equipment under control (EUC) to operate. Engaging the E-Stop beforehand ensures the system remains in a safe state until you explicitly disengage it.

1. Plug the power supply into an outlet.
2. Turn the docking station over and insert the USB-C connector into the port on the underside of the docking station:

Fig 4.2: Docking Station Underside

3. Push the WES Pro into the docking station until it clicks in place.

Fig 4.3: WES Pro in Docking Station

The WES Pro turns on (if off) and the indicator light on the docking station shows that it is charging. The LCD screen also shows the charge percentage for the battery.

4. Remove the WES Pro from the docking station when it's sufficiently charged.
5. When it's safe to do so, disengage the E-Stop by turning the button clockwise until it snaps out, which allows the EUC to operate normally. If the WES Pro is connected to a receiver and in range of it, when you disengage the E-Stop, the EUC powers on.

WES Pro Features and Operation

The following figure highlights the WES Pro Features: Top View should say Front View and add a back view that shows the belt clip.

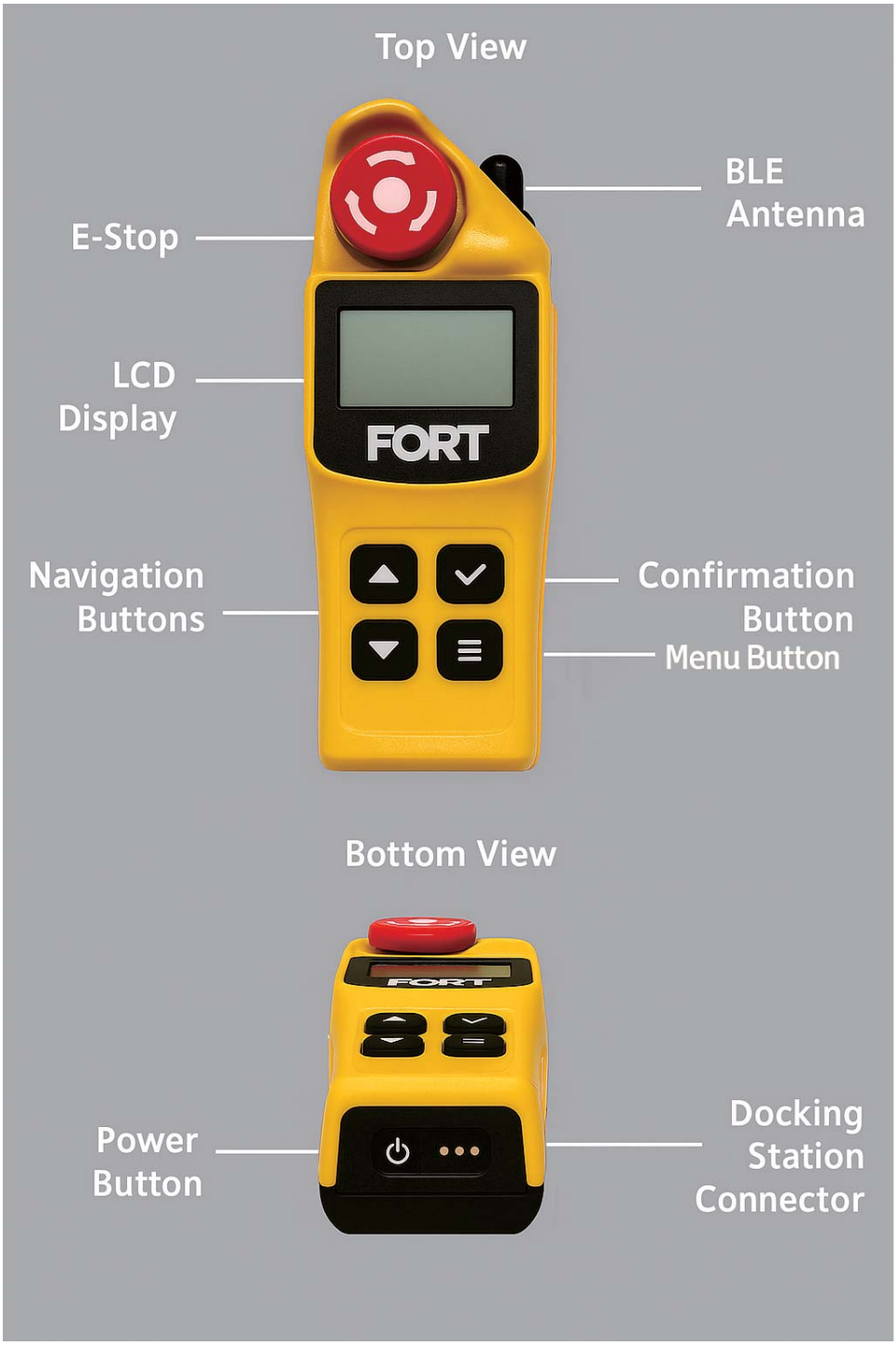

Fig 4.4: WES Pro Features

Turn WES Pro On or Off

Push the power button (located on the bottom of the device) to turn the WES Pro on or off. When you turn it on, the LCD screen lights up and the device vibrates when it is ready to use. Inserting the device into the docking station also turns it on if the docking station is connected to a power supply.

When you push the power button to turn it off, if the WES Pro is connected to a receiver, it stops sending valid safety

messages, which causes the connected device to go to the safe state after the timeout period is exceeded.

Caution

We recommend that you press the E-Stop button before powering the WES Pro on or off. When you turn the WES Pro back on, if in range, it automatically reconnects to the receiver, potentially triggering the EUC to operate. Engaging the E-Stop beforehand ensures the system remains in a safe state until you explicitly disengage the E-Stop.

Tip

Push and hold the power button (for 8 or more seconds, release it when the screen dims) to reboot the device.

E-Stop Button

Press the E-Stop button to send a safety command to a connected device or devices. The LCD displays an alert: I don't see this alert right away. It only appears if I turn the device off and back on.

```
E-Stop triggered for all connected machines DISENGAGE E-STOP
```

Press the check mark button to clear the alert.

Turn the E-Stop button clockwise until it pops out to disengage the E-Stop command.

Caution

Once you disengage the E-Stop, the connected devices will operate normally. Be certain that all machines in your configuration are safe to operate before disengaging the E-Stop.

WES Pro Menu Screen

Press the three-line Menu button to access the WES Pro menus:

- Press the up and down arrows to navigate between menus and between menu items.
- Press the check mark to open a menu or to change the setting for a menu item.
- Press the Menu button to move back a level in the menu structure.

Note

For some menus, you press the check mark or Menu button to exit, in which case, the menu instructs you to do so.

The WES Pro provides the following menus:

- **Receiver devices**: Lists lists all receivers to which the WES Pro is able to connect[1] . What happens when EPCs are offline? Is Receiver Devices simply reading the configuration. Can we shorten this to **Receivers**?
- **Device Attributes: Lists WES Pro device information, including:**
  - Serial Number - Shows the serial number for the device.
  - Firmware Version - Shows the version of the firmware that is running on the device.

[1] For this release, a WES Pro can pair with only one receiver. Consult the Release notes for information specific to the version of the product that you are using.

  - RSSI - (Received Signal Strength Indicator) as perceived by the WES Pro.
  - Battery Information - Shows the Volts, Amps, cycle count, and percentage remaining for the battery.
  - Config Name - Name of the configuration to which the device belongs.
  - MAC address
  - Radio Channel - Shows the radio channel. What does this show?
  - Radio Power - Shows the radio power level. Mine shows 0, does that mean there is no radio?
  - Hardware version - This is from JAMA but not showing on my WES Pro
- **Device Settings: The settings menu allows you to customize the following settings:**
  - Brightness - Set the display to low, medium, or high.
  - Haptics - Turn haptic responses on or off. The WES Pro provides three distinct vibration patterns to indicate device issues (low battery, communication loss, weak signal, etc.). Is that how this work, on or off?
  - Motor Test - Set the motor haptic response to Normal, Strong, or Pulse. Is that right? It seems to change after turning on and off?
  - Button Test - Allows you to verify that each of the buttons is responding when pressed.

Alerts

The WES Pro provides visual and haptic alerts: (does it? Do each of these alerts correlate to something on the LCD screen. Battery is shown, what about communication loss?) - It vibrates to indicate low battery (below 10%). - It vibrates if it shuts down due to low battery. - It vibrates if it loses communication with a receiver. - It vibrates to indicate a weak wireless signal. - The LCD displays an alert when an E-Stop is triggered:

```
E-Stop triggered for all connected machines DISENGAGE E-STOP
```

Turn the E-Stop button clockwise until it pops out to disengage the E-Stop command. Once you disengage the E-Stop, the connected devices will operate normally.

Connecting the WES Pro to an EPC

Once the configuration to which the devices belong has been uploaded to a WES Pro and to the EPCs in the configuration, the devices begin communicating withi each other as soon as they are turned on and are in range of each other.

Before You Begin

Make certain that

- You have uploaded the configuration to which the devices belong to all devices.
- All devices are powered up and in range of each other.

To Connect a WES Pro to an EPC:

1. Power up both devices and keep them within range of each other.
2. As a safety precaution, press the E-Stop button. (When you finish connecting to the new device, the E-Stop signal guarantees that the equipment won't start operating unexpectedly. The WES Pro displays a warning screen indicating that the E-Stop button has been pressed.
3. Press the **Check Mark** button to exit the E-Stop activated screen.

4. Press the **Menu** button and use the arrow keys to navigate to the **Receiver Devices** tab, then press the **Check Mark** to select it.

The screen shows a list of devices[2] that belong to the configuration in FORT Manager.

5. When it is safe to do so, turn the E-Stop button clockwise until it pops out to release it. At this point, you can press the E-Stop button at any time to send a safety signal to the connected EPC.

Connecting a WES Pro to a Configuration with an SRC Pro Controller

Probably need a procedure explaining how to connect in a hybrid environment WES Pro and SRC Pro.

Replacing the Battery

We recommend replacing the battery when the battery health indicator is at *x* % or lower What level do we recommend?

To check the battery health, press the **Menu Button > Device Attributes > Battery Health**. Is this right?

To Replace the Battery

[2] For the initial release, a WES Pro can pair with one receiver only. Consult the Release notes for information specific to the version of the product that you are using.

FORT provides a battery replacement kit. Do we have a part # and ordering info?

1. Use a phillips screwdriver to remove the four screws on the back panel of the WES Pro:

Fig 4.5: Back Panel WES Pro

2. Lift out the battery.
3. Insert the new battery.
4. Replace the back panel and tighten the screws.

Storing the WES Pro

If you plan to store the WES Pro for an extended period of time, we recommend doing so at the following temperatures to maximize battery life:

Table 4.1: WES Pro Recommended Storage Temperatures

Period	Temperature
Up to one month	-20 °C to 50 °C
One to three months	-10 °C to 45 °C
Longer than three months	-10 °C to 35 °C

APPENDIX

A

TECHNICAL SPECIFICATIONS

This appendix provides details of the Wireless E-Stop Pro (WES Pro) hardware.

Mechanical Overview

The following figure shows front and bottom views of the WES Pro:

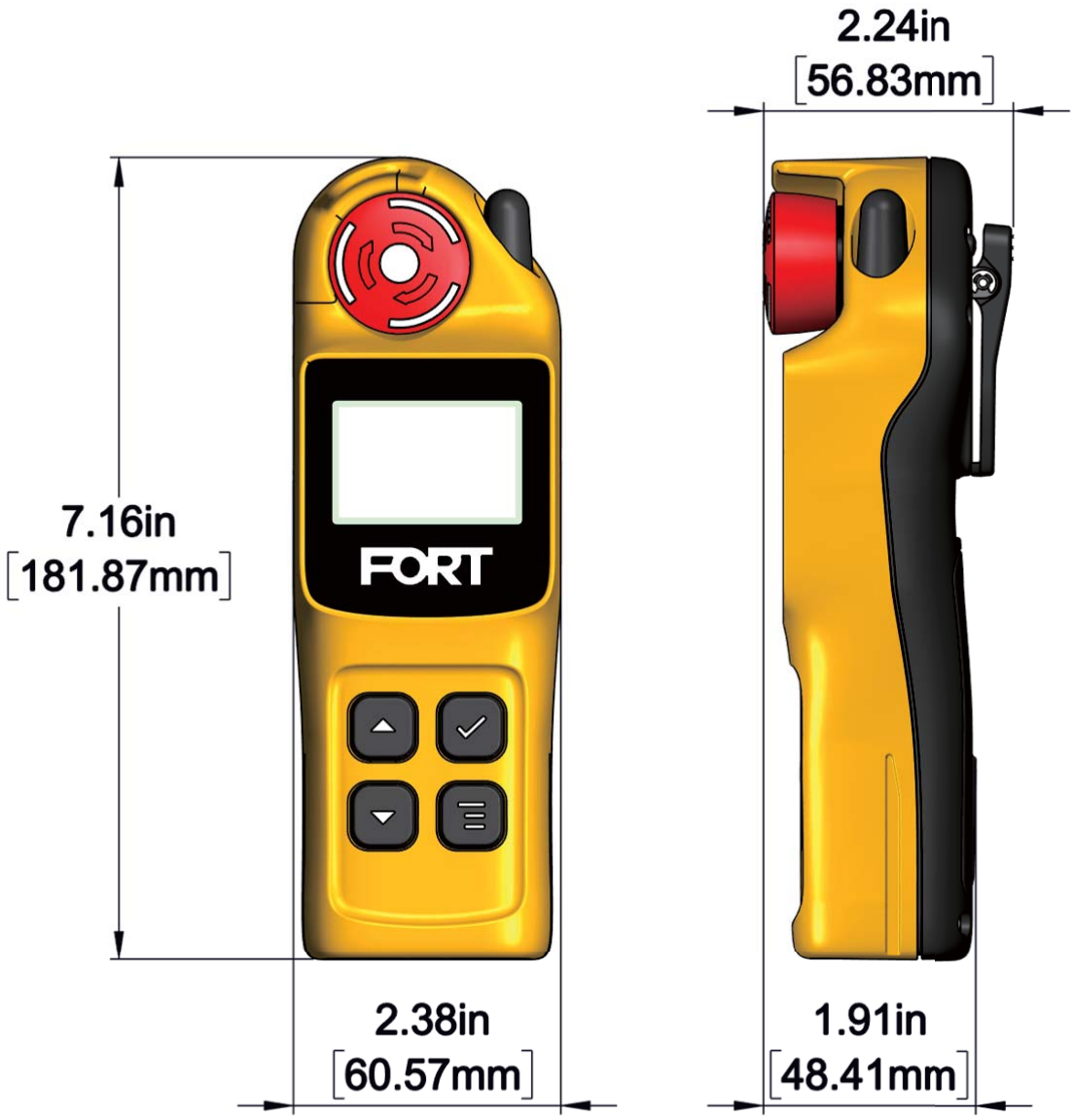

Fig A.1: WES Pro Front and Bottom

The following table shows details about the WES Pro.

Table A.1: WES Pro Specifications

Specification	Description
Device Form Factor	Wireless handheld sender
Dimensions	43 mm x 60 mm x 180 mm (1.69” x 2.36” x 7.09”)
Weight	450 g (0.992 lb)
Operating Temperature (internally limited)	-20°C to +60°C
Storage Temperature	Up to one month: -20 °C to 50 °C One to three months: -10 °C to 45 °C Longer than three months: -10 °C to 35 °C
Charging Temperature (internally limited)	0 °C-45 °C
Operating Voltage	4.5 to 13V DC input
Vin (V)	5 VDC (USB) @1.6 A
Ingress Protection WES Pro	IP65
Ingress Protection Docking Station	IP30
Output Radio Transmission Power (conducted RF output)	ISM: -10 dBM to 27 dBM ?no ism?
Battery Type & Size	Lithium, 1.5 A
Charge Time	4 hours or less
Run Time	12 hours or more
Power Draw	100 mW
Safety Outputs	One dual channel digital output
Pairing	1 WES Pro to 1 EPC[1] or 1 WES Pro + 1 SRC Pro to 1 EPC
Regulatory	Pending FCC, IC, CE compliant (US)(CA)(EU)
Certification	E-Stop SIL3 rated per IEC 61508 (pending)

Removed Extended Warranty from table. Verify that Guardian is gone. Verify Battery charging rate Is Vin @1.6A and Size 1.5A describing the same thing?

You can purchase a WES Pro with a long range Bluetooth radio[2].

[1] Be sure to check the the Release notes for information about the type and number of devices you can pair with a WES Pro that is specific to the version of the product you are using.

[2] Currently, the only radio available for the WES Pro is long range Bluetooth (LRBLE). Be sure to check the the Release notes for information about the type(s) of radios available for the WES Pro specific to the version of the product you are using.

Safety Output Specifications

The following table provides specifications for the safety outputs: These came from EPC, may or may not be accurate for WES Pro – Not in JAMA?

Table A.2: Safety Output Specifications

Specification	Description
PVin	4.5 V–13 V
Safety Outputs	One dual channel output
Output Type	Current Sourcing
Current (per output channel)	230 mA
Leakage Current (OFF state)	0.714 uA @8 V-0.892 uA @32 V
Output ON State	4.5 V-13 V Correct?
Output safe state	0, ?
OSSD Pulse Width	300 μS
OSSD Pulse Period	200 mS

Long-Range Bluetooth Low Energy (LRBLE) Radio (WES Pro)

The following table provides specifications for the WES Pro BLE radio:

Table A.4: BLE Radio Specifications (WES Pro)

Specification	Description
BLE Long Range Version	5.0
Tx Power (conducted RF output)	+20 dBm
Receive Sensitivity	-105 dBm From datasheet but RG thinks -80 might be more what it is – verify?
Range	100-300 m
Other	Any other specs that we want to show?

Important

We declare that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. This product can be used across EU member states.

APPENDIX

B

SAFETY

This Appendix explains the safety related operations and methods used to achieve functional safety of the Pro Series devices. This information shall be considered by the designated responsible individuals who would need and use the following information to properly apply to the Pro Series devices.

The only safety relevant function of a Pro Series device (an EPC, NSC Pro,SRC Pro, or WES Pro) is related to handling of the emergency stop (E-Stop) command.

A given EPC, based on how it is configured by the customer (using FORT Manager), can act as a sender that reads the safety input state and transfers each change in state (i.e., emergency stop requests) or it can act as a receiver that receives and acts on emergency stop requests.

An SRC Pro and WES Pro alway act as sender devices. An NSC Pro always acts as a receiver device.

The following sections of this chapter describe the operations inside the EPC, SRC Pro, NSC Pro, and WES Pro, including input, logic, and output, and explain in detail all valid use cases and their functional safety operations.

1oo2 Safety Architecture with HFT=1

The system comprising the hardware and software is designed using the redundant 1oo2 (one out of two) safety architecture approach.

To comply with the 1oo2 safety architecture, the system has two redundant safety hardware components on board the EPC, SRC Pro, NSC Pro, and WES Pro with their own independent input circuitry, processing, output circuitry, and internal monitoring (via a watchdog).

The processors on the two redundant safety subsystems also communicate with each other through a serial link.

The end-to-end redundant architecture used in the EPC, SRC Pro, NSC Pro, and WES Pro achieves a Hardware Fault Tolerance (HFT) of 1, as shown in the following diagram:

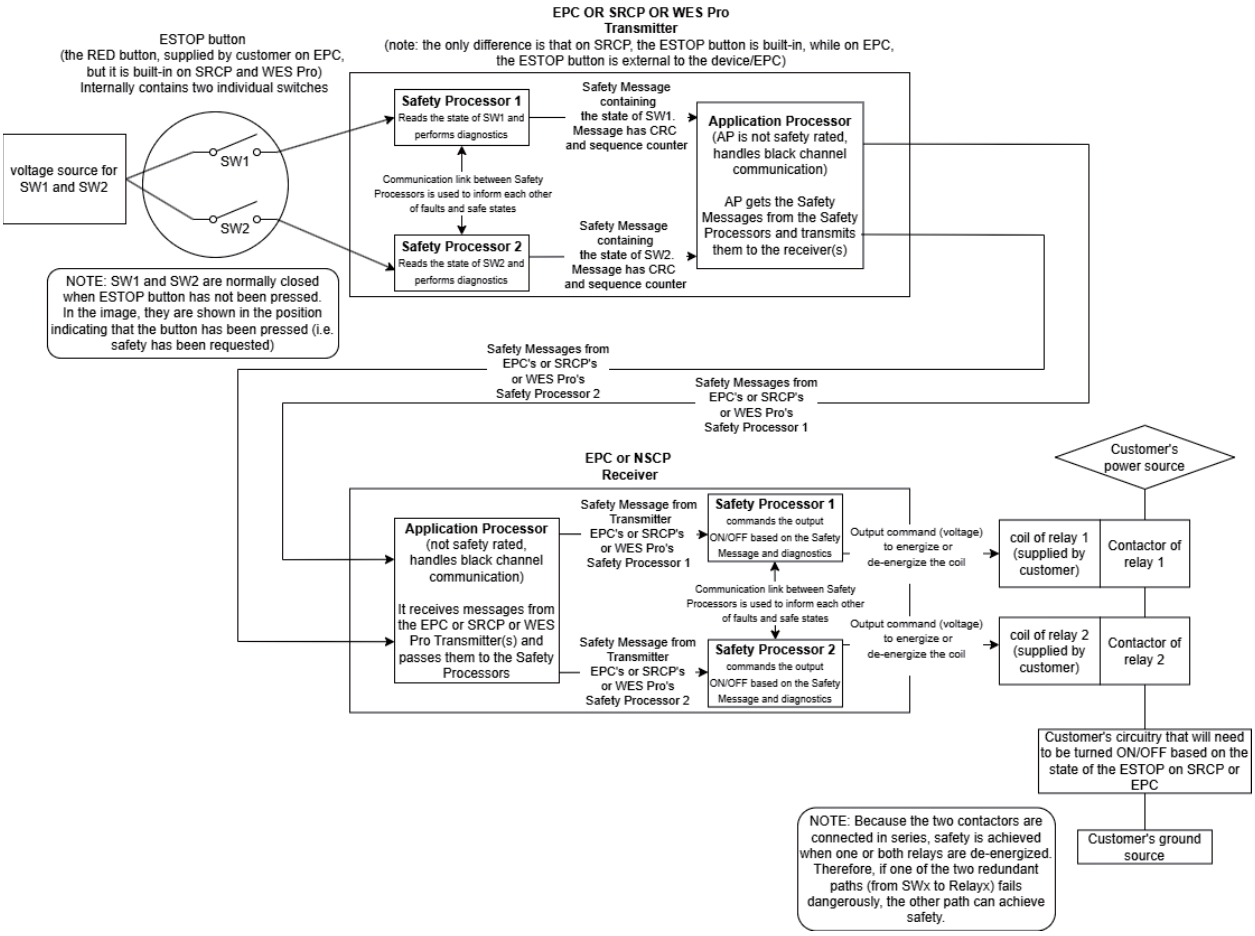

Fig B.1: 1oo2 Safety Architecture with HFT=1

If one channel stops communicating with the other channel for longer than a specified period of time, then the other channel enters a safe state as follows:

- A sending device (SRC Pro, EPC, or WES Pro) sends a safety message to request safety from the remote device(s).
- A receiving device (EPC or NSC Pro) turns off the relays or actuators that are connected to its outputs.

If either of the two channels encounters a failure, the system is not degraded from 1oo2 to 1oo1; rather, if one of the two channels goes to a safe state the other channel is designed to enter a safe state as well.

The system is designed as a fail-safe system whereby if the system loses power:

- A sending device (SRC Pro EPC, or WES Pro) stops transmitting safety messages which triggers a timeout on receiving EPCs or NSC Pros which then causes the receiving devices to turn off their output relays.
- A receiving device (EPC or NSC Pro) loses power (turns off) which causes all outputs to be open circuit, which in turn causes the connected output relays to turn off.

The two redundant safety subsystems communicate with an onboard non-safety subsystem that sends the safety request messages to and receives them from the safety processors. The non-safety subsystem (called Application Processor or AMCU) functions as part of the black channel communication and transfers the safety messages to and from SMCUs without modifying their content (Redundant with black channel requests).

If the AMCU changes the content of a safety message because of an error, the receiving SMCU will detect the change and will consider the changed message invalid and will not act upon it.

Safety Behavior of an EPC Sender

The external (customer supplied) sensing elements that are connected to the input(s) of the EPC, generate a signal that indicates whether safety has been requested. The EPC (more precisely: the safety processors of the EPC) reads these inputs, interprets them based on the voltage level of the signals, and then generates a safety request message that indicates whether safety is requested. The message is serially passed to the Application Processor (also known as the application microcontroller unit, AMCU) of the EPC.

The Application Processor takes the message and sends it to other receivers (EPCs or NSC Pros) via a communication link.

The AMCU of the receiving devices (EPCs or NSC Pros) receives the safety request messages and sends them serially to the onboard safety processors to be processed and acted upon.

Safety Behavior of an NSC Pro

The NSC Pro receives remote safety request messages from an SRC Pro or an EPC and depending on the request, turns on the relays (customer supplied) that are attached to its output (when the remote device doesn't request safety) or off (when the remote device requests safety). The receiver also checks the output feedback and confirms the output state.

Safety Behavior of an EPC Receiver

The EPC receives remote safety request messages from an SRC Pro, a WES Pro, or another EPC, and depending on the request, turns on the relays (customer supplied) that are attached to its output (when the remote device doesn't request safety) or off (when the remote device requests safety). The receiver also checks the output feedback and confirms the output state.

Safety Behavior of an SRC Pro

The safety behavior of SRC Pro is very similar to that of an EPC Sender.

The emergency stop switch that is built-into an SRC Pro generates a signal that indicates whether safety has been requested. The safety processors of the SRC Pro read this signal, interpret it based on the voltage level of the signal, and then generate a safety request message that indicates whether safety has been requested. The message is serially passed to the Application Processor of the SRC Pro.

The Application Processor receives the message and transmits it to a remote receiver EPC or NSC Pro via a supported communication link.

The AMCU of the receiving device (EPC or NSC Pro) receives the safety request message and sends it serially to the onboard safety processors to be processed and acted upon.

Safety Behavior of WES Pro

The safety behavior of WES Pro is very similar to that of an SRC Pro or EPC Sender.

The emergency stop switch that is built-into a WES Pro generates a signal that indicates whether safety has been requested. The safety processors of the WES Pro read this signal, interpret it based on the voltage level of the signal, and then generate a safety request message that indicates whether safety has been requested. The message is serially passed to the Application Processor of the WES Pro.

The Application Processor receives the message and transmits it to a remote receiver EPC or NSC Pro via a supported communication link.

The AMCU of the receiving device (EPC or NSC Pro) receives the safety request message and sends it serially to the onboard safety processors to be processed and acted upon.

Compliance with IEC 61508 requirements as a SIL-3 device

The emergency stop function is designed in compliance with SIL-3 requirements of IEC 61508.

Compliance with the IEC 61508 requires the system level requirements detailed in the following section.

> **Note**
>
> Although this document fulfills implied functional safety requirements in accordance with IEC 61508 and FORT Robotics engineering development processes, in the event of a conflict between the documents referenced and the contents of this guide, the current document applies.

Safety Inputs

An EPC (more precisely, the safety relevant portion of the EPC) provides support for processing and handling of two types of inputs: physical inputs and virtual inputs.

The SRC Pro and WES Pro support processing and handling of the built-in emergency stop switch.

Physical Inputs

This section describes the physical inputs for the EPC and SRC Pro.

EPC Physical Inputs

Physical input circuitry interfaces with the input devices (mechanical emergency stop switches, and more complex, solid state devices like a light curtain) that the customer connects to the EPC. The input circuitry conditions the input signals and provides them to the safety processors. Safety processors then calculate the magnitude of the signals to determine if safety has been requested or not.

Each EPC provides redundant hardware circuitry and the associated software to support the connection of three external physical input devices that have redundant outputs. The system reads and processes the state of each external physical input as an analog value using ADC (Analog to Digital Conversion) and checks the processed value of analog inputs against specified voltage ranges to determine whether the value of the signal indicates that safety has been requested.

The following external physical input devices are supported:

- E-Stop (Emergency Stop) type switches that are internally redundant (the E-Stop switch has two mechanical switches built inside it).
- Solid state type devices such as a light curtain, proximity sensor, etc., that must have redundant outputs.

If the solid state type device's signal includes a diagnostic off-pulse (known as OSSD), the system does not react to this pulse.

An input of an input-output pair only affects the output that it is paired with; for example, the input of input-output pair 1 can only affect the output of input-output pair 1 and cannot affect the output of input-output pair 2 or 3.

SRC Pro Physical Inputs

Physical input circuitry interfaces with the built-in mechanical emergency stop switch (which internally includes two individual SPST switches). The input circuitry conditions the input signals and provides them to the safety processors. Safety processors then calculate the magnitude of the signals to determine if safety has been requested or not.

The system reads and processes the state of the built-in E-Stop switch as an analog value using ADC (Analog to Digital Conversion) and checks the processed value of analog inputs against specified voltage ranges to determine whether the value of the signal indicates that safety has been requested.

WES Pro Physical Inputs

Physical input circuitry interfaces with the built-in mechanical emergency stop switch (which internally includes two individual SPST switches). The input circuitry conditions the input signals and provides them to the safety processors. Safety processors then calculate the magnitude of the signals to determine if safety has been requested or not.

The system reads and processes the state of the built-in E-Stop switch as an analog value using ADC (Analog to Digital Conversion) and checks the processed value of analog inputs against specified voltage ranges to determine whether the value of the signal indicates that safety has been requested.

Virtual Inputs

Virtual Inputs (applicable only to receiver EPCs or NSC Pros) are safety request messages, generated by the SMCUs of a remote EPC or SRC Pro, that are serially transmitted to the AMCU of the EPC or SRC Pro, which then transmits them using a wired or wireless link to the Application Processor of a remote EPC or NSC Pro.

The Application Processor of the remote EPC or NSC Pro receives the safety request message and then serially transmits the message to the SMCUs.

Serial Communication with Application Processor (AMCU)

On a sender EPC, SRC Pro, or WES Pro, only correct assembly of the safety message is considered safety relevant. Therefore, transmission of the safety request message to the AMCU is not safety relevant; however, if there is a failure in passing the message to AMCU, or if there is a failure on the AMCU side to transmit the message, the remote EPC or NSC Pro will go to safe state if this failure lasts longer than the timeout value.

On a receiving EPC or NSC Pro, if the AMCU doesn't pass the safety message to the SMCU, a timeout occurs that puts the outputs in a safe state. If the AMCU corrupts the safety request message, the CRC (cyclic redundancy check) and other checks by SMCU will detect the error and will not use the content of the message.

In summary: only assembling the safety message and processing the incoming safety request message is safety relevant. The rest of the communication chain is considered a black channel.

Serial Communication between the two Safety Processors (SMCU)

This is applicable to SRC Pro, NSC Pro EPC, and WES Pro. If one of the two channels of the 1oo2 system fails, the system must not degrade to 1oo1 operation. Therefore, when an SMCU detects an error and puts itself in a safe state, it must notify the other SMCU in order for the other SMCU to also go to a safe state. Therefore, the two SMCUs periodically communicate their state to each other by sending a message through a serial link.

Moreover, if an SMCU doesn't receive the periodic message from the other SMCU, after a specified period it goes to a safe state until it receives a valid safety message from the other SMCU.

This message uses the same approach to verify the message (CRC counter, and timeout) as the safety request message (see previous section) and the content of a message that fails the sequence counter check will not be used by the SMCU.

At least one valid message must be received by each SMCU from the other SMCU every timeout period (40ms), otherwise the outputs (both virtual and physical) are put in a safe state. Specifically, the system sends SMCU-to-SMCU messages every 10 ms (within every control loop), and if an SMCU doesn't receive a valid message from the other SMCU for four consecutive loops, it goes to a safe state.

When an SMCU receives a message from the other SMCU that indicates the other SMCU is in a safe state, the first SMCU also transitions to a safe state and puts all of its outputs (physical or virtual) in a safe state.

Timeout Period for Safety Request Message

The Application Processor of an EPC or NSC Pro receives the safety request message from a remote EPC, SRC Pro, or WES Pro, and using a serial link, transmits the message to the safety processors.

Before using any other field of the safety message for any purpose, the safety processors examine the content of the safety request message using the sequence counter and the CRC fields, to determine if the message is valid and has not changed during its transmission from the source to the destination.

At least one valid safety request message must be received by the SMCU within the timeout period since the last valid message, otherwise the outputs will be turned off to put the EUC in a safe state. For example, a safety timeout of 250 ms means that a receiver EPC or NSC Pro must receive at least one valid safety message within 250 ms of receiving the last valid safety message or else it will turn off its outputs.

The allowed timeout periods that can be chosen by the customer (using FORT Manager) are 250 ms, 500 ms, 750 ms and 1 sec, 3 sec, and 5 sec.

Safety Processing

To comply with the 1oo2 safety architecture and SIL requirements, the safety portion of the EPC, SRC Pro, NSC Pro,and WES Pro uses two redundant processing units, referred to as SMCU0 and SMCU1. Each double redundant input is connected to one of the SMCUs. For example, the double redundant E-Stop switch, internally contains two mechanical switches. One switch is connected to SMCU0 and 1 switch is connected to SMCU1.

Each safety processor reads the value of the input signal (virtual or physical) that it receives and based on the magnitude/content of the signal will command the physical outputs to either turn on or off or transmit a message indicating safety being requested or not.

The system complies with highly recommended safety requirements (the micro manufacturer refers to them as CoU, Conditions of Use) that are listed in the manufacturer's safety manual of the specific processor in use.

Important

When any of the safety mechanisms indicates the presence of a failure, the system logs a fault that indicates the reason for the fault, and it places the outputs (both virtual and physical when applicable) in a safe state.

Safety Outputs

This section describes the safety outputs for the EPC, NSC Pro, SRC Pro, and WES Pro.

EPC Safety Outputs

An EPC provides support for processing/handling of two types of outputs: physical outputs and virtual outputs.

An EPC sender provides support for three virtual outputs that indicate the state of the 3 physical inputs of the EPC sender.

An EPC receiver provides support for three redundant and independent physical outputs.

The user must configure the outputs with FORT Manager.

NSC Pro Safety Outputs

An NSC Pro provides support for processing/handling of physical outputs.

Each NSC Pro has two redundant and independent physical outputs.

The outputs must be configured by the user, using FORT Manager.

SRC Pro Safety Outputs

The SRC Pro is a transmitter device and therefore only supports one virtual output that indicates the state of the built-in emergency stop switch.

WES Pro Safety Outputs

The WES Pro is a transmitter device and therefore only supports one virtual output that indicates the state of the built-in emergency stop switch.

Physical Outputs

Physical outputs are only applicable to receiver EPCs and NSC Pros. Physical output circuitry creates a link between the safety processor and the output devices, which are typically relays (or actuators) that a user connects to the outputs of the EPC or NSC Pro. Based on the state of the inputs and the safety system's diagnostics information, the safety processors determine whether the relays need to be turned on or off.

For example, if the state of inputs indicates that safety has been requested, the system turns off the outputs to turn off the external relays, otherwise it keeps the outputs on to keep the external relays on.

Each EPC provides redundant hardware circuitry and the associated software to support the connection of three external and redundant physical output devices. The external physical output devices must be connected in series, such that if one or both of the two devices are turned off, the EUC is turned off.

Each NSC Pro provides redundant hardware circuitry and the associated software to support the connection of two external and redundant physical output devices.

If the state of any virtual input indicates that safety has been requested by a remote device, the output of that device is turned off.

If the system has a fault that could affect all of the outputs, all the outputs will be turned off.

Virtual Outputs

Virtual outputs are applicable to SRC Pros, Sender EPCs, and WES Pros. Virtual outputs are safety request messages generated by the SMCUs of an EPC, SRC Pro, or WES Pro, based on the state of the physical inputs and diagnostics information. Every 40ms these messages are serially transmitted to the AMCU of a transmitting EPC,SRC Pro, or WES Pro, which then transmits them using a wired or wireless link to the Application Processor (AMCU) of a remote EPC or NSC Pro that is connected to a machine. The Application Processor of the remote device receives the safety request message and serially transmits it to its SMCU. See diagram in *1oo2 Safety Architecture with HFT=1*

The AMCU acts as part of a black channel and does not deliberately modify the content of the safety request message. The CRC verification detects accidental corruption of the message at the destination.

The content of the safety request message also includes a sequence counter that is incremented as each new message is transmitted to the AMCU. This enables the remote device to detect out of sequence and old messages that it must not act upon.

The following information is applicable to an EPC and NSC Pro, not to an SRC Pro.

User Selectable Safety Configurations (EPC)

A user must configure an EPC with FORT Manager before the device can be used in a runtime application. See *Configurations and Use Cases (WES Pro)*. A subsequent power cycle of the EPC does not erase the configuration stored in the device. Any re-configuration of an EPC must be done by a user with FORT Manager.

Use FORT Manager to configure the EPC, including the inputs and outputs of the safety portion of the EPC:

- Configuration: Identify the sender(s) and receivers for the network.
- Timeout Configuration: Select one of the values 250ms, 500ms, 750ms, 1 second, 3 seconds, or 5 seconds as a timeout.
- Input configuration: Identify the type of device (E-Stop, solid-state, or not used) to attach to each of the three inputs.
- Output configuration: Derived by FORT Manager from the configuration information entered by the user.

User Selectable Safety Configurations (NSC Pro)

The following information is applicable to an NSC Pro only.

A user must configure an NSC Pro with FORT Manager before the device can be used in a runtime application. A subsequent power cycle of the NSC Pro does not erase the configuration stored in the device. Any re-configuration of an NSC Pro must be done by a user with FORT Manager.

Use FORT Manager to build a configuration and to configure the NSC Pro, including the outputs of the safety portion of the NSC Pro:

- Configuration: Identify the sender(s) and receivers for the network.
- Timeout Configuration: Select one of the values 250ms, 500ms, 750ms 1 second, 3 seconds, or 5 seconds as a timeout.
- Input configuration: Identify the type of device (E-Stop, solid-state, or not used) to attach to each of the three inputs.
- Output configuration: Derived by FORT Manager from the configuration information entered by the user.

User Selectable Safety Configurations (WES Pro)

Using FORT Manager, a user must configure which output of the receiver will be controlled by the ESTOP on WES Pro.

Transferring Safety Configurations from FORT Manager to the EPC

When a user configures an EPC with FORT Manager, FORT Manager is not in direct communication with the EPC that is being configured. Therefore, FORT Manager stores the configuration parameters in a file that the user later transfers to the AMCU with the FORT configuration tool or the FORT Manager desktop app.

After each reset or power up, the SMCU of the EPC retrieves the configuration parameters from the AMCU.

To ensure that program file corruption or an accidental change of configurations can be detected, FORT Manager calculates a CRC for SMCU configurations that it transmits to the AMCU and includes as part of the SMCU configuration data. Upon completion of transfer of the configuration to its RAM, the SMCU verifies that the CRC of the configuration matches its content, and if not, logs a fault and resets the SMCU.

After an SMCU receives its configuration, it verifies that the configuration is one of the allowed configurations. If it isn't, the SMCU resets itself and the EPC cannot enter a running state of operation.

Transferring Safety Configurations from FORT Manager to the WES Pro

When a user configures an WES Pro with FORT Manager, FORT Manager is not in direct communication with the WES Pro that is being configured. Therefore, FORT Manager stores the configuration parameters in a file that the user later transfers to the AMCU with the FORT configuration tool or the FORT Manager desktop app.

After each reset or power up, the SMCU of the WES Pro retrieves the configuration parameters from the AMCU.

To ensure that program file corruption or an accidental change of configurations can be detected, FORT Manager calculates a CRC for SMCU configurations that it transmits to the AMCU and includes as part of the SMCU configuration data. Upon completion of transfer of the configuration to its RAM, the SMCU verifies that the CRC of the configuration matches its content, and if not, logs a fault and resets the SMCU.

After an SMCU receives its configuration, it verifies that the configuration is one of the allowed configurations. If it isn't, the SMCU resets itself and the WES Pro cannot enter a running state of operation.

Mechanical and Electrical Safety (EPC)

The EPC is designed and built to operate in extreme environmental conditions. As such, we've subjected it to rigorous mechanical and electrical tests.

Humidity and Dust Restrictions (EPC)

The EPC has no humidity restrictions (tested to MIL-STD-810H) or dust restrictions (IP65 verified).

Vibration Restrictions (EPC)

The EPC meets vibration standards per SAE (Society of Automotive Engineers) J1455. It was subjected to 8.00 G-rms of random (Gaussian) vibration for six hours each in three separate planes with results as shown in the following table:

Table B.1: Vibration Power Spectral Density (PSD) Results (EPC)

Frequency (Hz)	PSD (G^2/Hz)
24	0.040
60	0.500
102	0.500
300	0.010
2000	0.010

Drop Restrictions (EPC)

The EPC has been tested by dropping from a height of one meter. It should continue to function after occasional drops but avoid dropping it repeatedly to prevent damage and malfunctioning.

Water Restrictions (EPC)

The EPC enclosure is IP65 rated (protected against exposure to water including low pressure sprays). Do not subject it to high pressure nor immersion in water. Note that if the EPC is operating in an environment in which it is exposed to water you must mount it vertically. Mounting it horizontally allows water to pool and block a breathable membrane causing the device to malfunction.

Proof Test (EPC)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition.

Based on your application, you should determine how frequently you must perform a proof test on the system.

See *Proof Testing* for a couple of suggested proof tests.

Mechanical and Electrical Safety (NSC Pro)

The NSC Pro is an embedded board that is designed and built to operate in extreme temperature ranges (-40 °C -85 °C). We've subjected it to the following tests:

Table B.3: NSC Pro Environmental Tests

Test Type	Standard	Parameters
Humidity	IEC 60068-2-78:2012	30±2°C; 0 – 93 ±3% relative
Thermal Cycling	IEC 60654-1	-40°C to +85°C (
Swept Sinusoidal Vibration Test	IEC 60068-2-6	Frequency range: 55-500 Hz; Acceleration amplitude: 6g; 10 swee
Shock	IEC 60068-2-27	25g acceleration; 6ms pulse duration; Half-sine pulse sha
Ingress Protection	IEC 60529	IP00
Radiated Emissions, Near Field	EC-42 Test 4.1/ISO 13766	
High Frequency Immunity	EC-42 Test 3.1	30V/m, ISO
Medium Frequency Immunity	EC-42 Test 3.2	30V/m ISO 11452-2, ISO
Low Frequency Immunity	EC-42 Test 3.3	30V/m, ISO 11452-4
Functional Safety	IEC 61508	Up to

Proof Test (NSC Pro)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition.

Based on your application, you should determine how frequently you must perform a proof test on the system.

See *Proof Testing* for a couple of suggested proof tests.

Mechanical and Electrical Safety (SRC Pro)

The Safe Remote Controller Pro is designed and built to operate in extreme environmental conditions. As such, we've subjected it to rigorous mechanical and electrical tests.

Humidity and Dust Restrictions (SRC Pro)

The SRC Pro has no humidity restrictions (tested to MIL-STD-810H) or dust restrictions (IP65 verified).

Vibration Restrictions (SRC Pro)

The SRC Pro meets vibration standards per SAE J1455. It was subjected to 8.00 G-rms of random (Gaussian) vibration for two hours each in three separate planes with results as shown in the following table:

Table B.5: Vibration Power Spectral Density (PSD) Results (SRC Pro)

Frequency (Hz)	PSD (G^2/Hz)
20	0.010
80	0.040
350	0.040
2000	0.007

Drop Restrictions (SRC Pro)

The SRC Pro has been tested by dropping from a height of one meter once on each side of the device. It should continue to function after occasional drops but avoid dropping it repeatedly to prevent damage and malfunctioning.

Water Restrictions (SRC Pro)

The SRC Pro enclosure is IPx5 rated (protected against exposure to water including low pressure sprays). Do not subject it to high pressure nor immersion in water.

Proof Test (SRC Pro)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition. Based on your application, you should determine how frequently you must perform a proof test on the system. See *Proof Testing* for some suggested proof tests.

Mechanical and Electrical Safety (WES Pro)

The WES Pro is designed and built to operate in extreme environmental conditions. As such, we've subjected it to rigorous mechanical and electrical tests.

Humidity and Dust Restrictions (WES Pro)

The WES Pro has no humidity restrictions (tested to MIL-STD-810H) or dust restrictions (IP65 verified).

Vibration Restrictions (WES Pro)

The WES Pro meets vibration standards per SAE J1455. It was subjected to 8.00 G-rms of random (Gaussian) vibration for two hours each in three separate planes with results as shown in the following table:

Table B.6: Vibration Power Spectral Density (PSD) Results (WES Pro)

Frequency (Hz)	PSD (G^2/Hz)
20	0.010
80	0.040
350	0.040
2000	0.007

Drop Restrictions (WES Pro)

The WES Pro has been tested by dropping from a height of one meter once on each side of the device. It should continue to function after occasional drops but avoid dropping it repeatedly to prevent damage and malfunctioning.

Water Restrictions (WES Pro)

The WES Pro enclosure is IPx5 rated (protected against exposure to water including low pressure sprays). Do not subject it to high pressure nor immersion in water.

Proof Test (WES Pro)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition. Based on your application, you should determine how frequently you must perform a proof test on the system. See *Proof Testing* for some suggested proof tests.

FMEDA Summary (EPC)

This section summarizes the expected failure rates for the EPC obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

The following two tables list the failure rates for the EPC using a site safety index (SSI) of 2 (good site maintenance practices).

Table B.7: EPC Failure Rates (Sender) Good Maintenance Assumptions in FIT @SSI=2

Failure	Category	Failure Rate (FIT)

Fail Safe Detected	9,034
Fail Safe Undetected	120
Fail Dangerous Detected	9,558
Fail Dangerous Undetected	92
No Effect	499
Annunciation Detected	34
Annunciation Undetected	23

Table B.9: EPC Failure Rates (Receiver) Good Maintenance Assumptions FIT @SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	9,030
Fail Safe Undetected	178
Fail Dangerous Detected	9,534
Fail Dangerous Undetected	92
No Effect	544
Annunciation Detected	50
Annunciation Undetected	23

The following table lists the failure rates for the EPC according to IEC 61508.

Table B.11: EPC Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration	λSD	λSU	λDD	λDU	#	SFF
Sender	9,067	120	9,558	92	522	99.5%
Receiver	9.080	178	9,534	92	567	99.5%

Where:

λSD = Fail Safe Detected **λSU** = Fail Safe Undetected **λDD** = Fail Dangerous Detected **λDU** = Fail Dangerous Undetected **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010.

The analysis shows that the EPC has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

FMEDA Summary (NSC Pro)

This section summarizes the expected failure rates for the NSC Pro obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

Note

Note: The failure rate tables make the assumptions that the altitude/SER is 200 m, failure rates apply to the NSC Pro only, and external components (E-Stop switch and safety relays) are not covered.

The following table lists the failure rates for the NSC Pro using a site safety index (SSI) of 2 (good site maintenance practices).

Table B.13: NSC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2

Failure	Category	Failure Rate (FIT)
Fail	Safe Detected	588
Fail	Safe Undetected	76
Fail	Dangerous Detected	547
Fail	Dangerous Undetected	9
No	Effect	266
Annunciation	Detected	39
Annunciation	Undetected	7

The following table lists the failure rates for the NSC Pro according to IEC 61508.

Table B.15: NSC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration		λSD	λSU	λDD	λDU	#	SFF
NSC	Pro	627	76	547	9	273	99.3%

Where:

- **λSD** = Fail Safe Detected
- **λSU** = Fail Safe Undetected
- **λDD** = Fail Dangerous Detected
- **λDU** = Fail Dangerous Undetected
- **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010.

The analysis shows that the NSC Pro has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

FMEDA Summary (SRC Pro)

This section summarizes the expected failure rates for the Safety Remote Control Pro obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

The following table lists the failure rates for the EPC using a site safety index (SSI) of 2 (good site maintenance practices).

Table B.17: SRC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2

Failure	Category	Failure Rate (FIT)
Fail	Safe Detected	4779
Fail	Safe Undetected	64
Fail	Dangerous Detected	5021
Fail	Dangerous Undetected	52
No	Effect	649
Annunciation	Detected	33
Annunciation	Undetected	13

The following table lists the failure rates for the SRC Pro according to IEC 61508.

Table B.19: SRC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration	λSD	λSU	λDD	λDU	#	SFF
SRC Pro	4811	64	5021	52	662	99.5%

Where:

λSD = Fail Safe Detected
λSU = Fail Safe Undetected **λDD** = Fail Dangerous Detected **λDU** = Fail Dangerous Undetected **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010

The analysis shows that the SRC Pro has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

FMEDA Summary (WES Pro)

Important

FMEDA testing for the WES Pro is in the works and this section will be updated when the results are in.`

Diagnostic Test Intervals

The diagnostic test interval (DTI) is the interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage. The DTI for EPC, NSC Pro, SRC Pro, and WES Pro is 50 milliseconds.

All the EPC, NSC Pro, SRC Pro, and WES Pro safety software (including diagnostic checks) run within a 10 ms control loop (except the Short-to-Battery test, which runs every 200 ms). However, not all online tests run every 10 ms and for those that do run every 10 ms, the software does some filtering on the faults to avoid the system entering a safe

state unnecessarily. Because of filtering some tests may take up to 50 ms to determine that a fault exists. In addition, some tests, such as the flash test, comprise five parts such that a complete flash test takes five control loops (50 ms) to complete.

For example, the two safety processors (SMCU0 and SMCU1) exchange information about their state every 10 ms via serial messages. However, they enter a safe state whenever either of the following occurs:

- They haven't received a valid status message for four consecutive control loops (i.e., 40 ms) from the other SMCU.
- They receive a valid safety message from the other SMCU indicating that it has entered a safe state.

The following table provides a summary of the diagnostic tests that are performed on the inputs, outputs, and internal parts of the system, how frequently they are performed, whether there is filtering, and the criteria for declaring a fault (i.e., entering a safe state).

Table B.21: Diagnostic Tests

Test name / Description	Applicability	What it does	How often it runs
State of Inputs Checks the state of the E-Stop switch(es) or the solid state input device(s) for faults.	Sender EPC, SRC Pro, and WES Pro	Checks whether the state of the switch/input indicates a fault. If the test fails, the output is turned off until the fault goes away.	Every 10 ms to sample the state of the input
Output Command to State Comparison Compares the output command(s) to the state of the output pin(s).	Receiver EPC or NSC Pro	Checks whether the voltage level at the output pin corresponds to the output command. If the test fails, the corresponding output is turned off until the system is reset.	Every 10 ms to make the comparison.
Short to Battery Checks whether a short to battery exists at the output pin(s) while the output(s) is commanded on (i.e., safety is not being requested). This test prevents a scenario in which, over a long period of time (potentially many months), and while safety is not being requested, both outputs are shorted to battery without the system being aware of the failure. If this scenario were to occur, and safety is requested at some point, a safe state cannot be achieved since both outputs have been shorted to battery.	Receiver EPC or NSC Pro	While safety is not being requested, the test momentarily (for less than 0.5 ms) turns off the output to check if the output indeed turned off (i.e., there is no failure) or if the output remains on (a short to battery is present). If the test fails, the corresponding output is turned off until the system performs a reset.	The test runs every 200 ms. This value is not used for DTI since it is a special test to prevent *double-point failures*, and the *Output Command to State Comparison* test performs a similar check every 10 milliseconds. There is no filtering of the test result.
Communication Timeout Checks whether a communication timeout exists between the sender and receivers. The scope of this test is limited to the safety request message.	Receiver EPC or NSC Pro	Checks whether a new and valid safety message has been received from each expected sender (could be an EPC or SRC Pro or both in the case of a hybrid configuration) since the last timeout period (as set by the user in FORT Manager). If a timeout is detected, the outputs are turned off until a valid safety message is received.	Checks the timeout counter(s) every 10 ms for a timeout.
Safety Processors Communication Timeout Checks for communication timeout between the two redundant safety processors	Sender EPC, SRC Pro, WES Pro, and Receiver EPC, NSC Pro	Run by each safety processor to check if it is receiving safety data from the other safety processor. Each safety processor must receive a safety message from the other processor at least every 40ms. If a timeout is detected, the outputs are turned off until a valid safety message is received.	Every 10ms each safety processor checks timeout counter for communication between safety processors.
Other internal diagnostics Each safety processor runs a series of checks on the health of the system such as ADC, RAM, FLASH, CPU, etc.	Sender EPC, Receiver EPC, NSC Pro, WES Pro	Each safety processor runs a series of tests to ensure that the subsystems of each processor are working correctly. The tests are based on the requirements of the safety manual of the safety processors. If a test fails, the system resets. During the reset, the outputs are forced OFF by the hardware.	Every 10ms.

APPENDIX

C

PRODUCT MAINTENANCE

This appendix explains

- How to care for your devices (next section)
- How to handle a device that is damaged or fails for any reason (*Troubleshooting*).
- How to proof test your devices and configurations (*Proof Testing*).
- How to update the firmware as necessary (*Updating WES Pro Firmware*).

Care and Handling

The WES Pro is designed and built to operate in extreme environmental conditions and as such, has been subjected to rigorous mechanical and electrical tests.

Keep the following points in mind when handling your devices:

- You can safely operate the WES Pro in a humid or dusty environment without fear of damaging the device.

> **Warning**
>
> Do not charge the device in a humid or dusty environment. Wipe off the docking station with a towel, if it is wet, before inserting the WES Pro.

- You can operate the WES Pro in the rain.
- The WES Pro is able to withstand an occasional drop from a height of one meter or less onto a hard surface, however, be careful not to drop it repeatedly. Although durable, it is not unbreakable, so be careful not to set it down and accidentally run over it with heavy equipment.
- You can clean it with a mild detergent and cloth.

> **Caution**
>
> Do not apply harsh chemicals to clean the WES Pro. Do not immerse it in water, avoid spilling liquids on it (wipe off immediately if this happens), and do not subject it to intense water jets.

Troubleshooting

Caution

The WES Pro has no user-serviceable parts, other than the battery. Do not attempt to make any changes or repairs to this device other than replacing the battery. If you have maintenance or repair questions fill out a request on the Customer Support Portal.

If a device fails for any reason, do the following:

- Discontinue use.
- Reboot the device.

If rebooting does not resolve your issue, fill out a request on the Customer Support Portal to address the issue. In the meantime, to keep your system functioning, you can use FORT Manager to replace the damaged device in your network if you have another device available. See *Configurations and Use Cases (WES Pro)*.

Proof Testing

Before integrating WES Pro with your work environment — and at periodic intervals — you must perform some basic safety (proof) tests to detect dangerous hidden failures in the EPC's safety system. If the proof test detects any failures, you must perform immediate repairs to restore the system to its as new condition or as close to as new as possible.

Based on your application, you should determine how frequently you must perform a proof test on the system.

Warning

Safe operation of the system requires that you thoroughly test the system before putting it into a production environment. Testing includes training your personnel on both the manual functions (pressing an E-Stop button, verifying menu settings, clearing faults, etc.) as well as automatic functions of the system (exceeding the timeout value, loss of radio signal, etc. triggering safety).

We recommend separate tests for an EPC to EPC configuration and for a WES Pro to EPC configuration, but you need to develop specific tests for each of your configurations as well.

To Proof Test WES Pro to EPC Configuration

To verify that outputs connected to a receiver EPC are working correctly and can cause an emergency stop on demand, perform the following procedure:

1. While the WES Pro is up and running, be certain that one or more EPCs[1] in the configuration are running.
2. While safety is not being requested, verify that the contactors on the receiver EPC are all closed.

   If any of the contactors is open, investigate and identify the source of the failure.

3. Request safety by pressing the E-Stop button on the WES Pro and verify that both contactors on the relay connected to the receiver EPC are open. If one or both contactors are not open, which indicates a failure, inspect the wiring and the relays to find the source of the failure. 4. Remove the request for safety on the WES Pro and verify that the devices are up and running.

Repeat this procedure for each EPC in the configuration.

[1] For the initial release, a WES Pro can pair with one receiver only. Consult the Release notes for information specific to the version of the product that you are using.

Wireless Communication Loss

A wide range of events can cause loss of signal events; for example, moving the WES Pro out of range of the EPC, introducing enough interference or obstructions, turning it, or anything else that prevents communication between the devices (such as improper antenna placement for the EPC receiver).

During normal operation, a receiver EPC expects to receive at least one valid safety message from the sender within the (user-configurable) timeout period or else it enters the safe state (turns off its outputs). If the receiver stops receiving valid messages because of communication loss (or any other reason), once the timeout period is exceeded, the safety processor on the EPC opens the safety relays to initiate the E-Stop command.

While performing safety tests on your Pro Series devices, verify that communication loss isn't affecting the performance of your equipment or causing unsafe operation. You can experiment with different values for the timeout while testing to address any issues you find. You set the timeout value in FORT Manager when building a configuration. See *Configurations and Use Cases (WES Pro)*.

A higher value, which makes the EPC less sensitive to communication loss, means that if a device loses communication with its sender, the EUC will run for a longer period before stopping automatically. On the other hand, a lower timeout value, which reduces the risk of the EUC running without connection to the safety controller, increases the sensitivity to communication loss.

Warning

FORT Manager provides a timeout of 250 msec that you can use for testing. Once you put your system into production, we strongly recommend that you do not keep this value as it has been shown to lead to frequent unstable communication. Consult with your system safety manager before using this timeout value.

Updating WES Pro Firmware

FORT releases periodic updates to the WES Pro firmware for performance, safety, and security reasons.

FORT Manager displays a message on the Dashboard page whenever new firmware is released. You can also navigate to the Firmware page to see the latest version that is available for each type of device. Compare the version in FORT Manger to the version on your device:

On the WES Pro, press **Menu Button > Firmware Version** and note the version.

Note

If you are not sure whether your firmware is up to date, or if you are eligible for updates, fill out a request on the Customer Support Portal or on the Dashboard page of FORT Manager (Submit Request) to get help. Is this relevant? Guardian is gone, does this mean everyone is eligible for all updates?

Important

Non-safety critical firmware updates are only available to customers whose device has an active Guardian subscription. Guardian allows you to get firmware and software updates, extended support, and warranty coverage beyond the limited one-year hardware warranty term. Guardian is no longer offered so what is our end-user agreement now?

If the firmware is out of date, you can access the firmware interface of the WES Pro in either of the following ways:

- By using the FORT Manager Desktop application (see *Updating the WES Pro Firmware with Desktop App*).

- By using the CLI tool (see *Updating the WES Pro Firmware with the CLI Tool*).

Updating the WES Pro Firmware with Desktop App

This section explains how to update the WES Pro firmware with the FORT Manager Desktop App. Note that this is the *Desktop* app, not the *Web* app; if you don't already have it, you can download the Desktop app, Windows or Linux version, from the Web app or directly from GitHub.

The next section explains how to use the CLI tool to update the firmware.

To Update Firmware using FORT Manager Desktop App

Required Items:

- A newer firmware version is available.
- Windows or Linux computer running with Ethernet networking capability (required for using the FORT Manager Desktop app).
- FORT Manager Desktop app (find latest version in FORT Manager Web app or at GitHub).
- The WES Pro is in a safe state.

1. Launch the FORT Manager Desktop app on your computer.
2. Connect the WES Pro docking station to a USB port on your computer (connect USB cable to USB C port on underneath of docking station).
3. Place WES Pro in the docking station (it turns on automatically). The application displays a message that it has detected a device for tethering. If multiple devices are connected to the computer, the application displays a list of devices to choose from.

> **Note**
>
> If the device is not automatically detected, click **Tether a Device** in the left pane, select **WESP** as the type of device, enter the port in **Path** (generally *COM3*), and click **Connect**.

4. Select the device and click **Tether**. The application displays information about the device including the firmware version. A yellow `New Update` badge next to the firmware version indicates that a newer version is available to update.
5. Click **Update** next to **Firmware** to upload the firmware to the device.

> **Important**
>
> Do not interrupt the update process once it begins. It takes approximately two minutes.

Once the update process finishes, the application untethers and reboots the device. The update badge turns green, displays `Updated` and the app shows the last sync date.

You can unplug the device from the computer unless you have a configuration update to apply as well.

To Download Firmware for Offline Loading

One of the advantages of the desktop app is that you can use it without an internet connection. If you plan to load configurations or make firmware updates when the internet is not available, you can download the firmware and configurations when connected to the internet and store them in the app for later retrieval.

> **Note**
>
> Downloaded files are stored in the application, not in the computer's file system, which means you access them through the Desktop app, *not* in the downloads file on your computer.

1. Launch the FORT Manager Desktop app on your computer.
2. Click **Firmware**.
3. Click **Download Configuration**.

The Download Status changes to *Downloaded*.

Updating the WES Pro Firmware with the CLI Tool

This section shows how to update firmware on a WES Pro in the field.

Required Items

- Linux computer running Ubuntu 20.04 with Ethernet networking capability or a Windows machine. Use USB_C to USB-A cable to connect your computer directly to the WES Pro docking station.
- Firmware upgrade file for the WES Pro. You can download an archive package that contains the latest version from FORT Manager (following procedure).
- Latest FORT CLI Configuration Tool (`fort_cli_cfg`). If you don't already have this tool, you can download it from FORT Manager.

To Download the WES Pro Firmware Upgrade File

(Requires DeviceManager or Admin role.)

1. Launch FORT Manager and enter your username and password when prompted.
2. Click **Firmware** in the left navigation pane to open the Firmware page.
3. Click the version number link in the **Current Version** column for the WES Pro (WESP).

   FORT Manager downloads the firmware update file to the Downloads folder on your computer. The file is in a compressed format but note that you don't need to uncompress it to install it.
4. (Optional, this step is required only if you are running FORT Manager in a browser on a different computer than your Linux computer, for example, on a Windows machine. If you are running FORT Manager on a Linux machine, you can skip this step.)

   Copy the file from a directory on your Windows machine to the home directory on your Linux computer by using the secure copy command (`scp`):

   a. Open a terminal on a Windows machine.

   b. Type the following (replace the values in brackets with your values):

   ```
   scp C:\<myDir>\<device_firmware_file> <user>@<ipaddress>:/home/<user>
   ```

Go to the next procedure to install the firmware file.

To Upgrade the WES Pro Firmware:

(Requires Admin or Operator role)

1. Connect the USB port on the WES Pro docking station (underneath) to your Linux computer.
2. Open a terminal and execute the FORT CLI Configuration Tool:

   Note that you need execute permission to `/dev/ttyACM0`.

```
fort_cli_cfg -n /dev/ttyACM0 -m
```

Where:

`-n (nxp) /dev/ttyACM0` Specifies a WES Pro device and identifies the USB port in use; your port could be different.

`-m (--menu)` Specifies the interactive menu option for the configuration tool

3. Use the arrow keys to navigate to **Device Firmware** and press **Enter**.
4. Use the arrow keys to navigate to **Device firmware** file data and press **Enter**.
5. Use the arrow keys to navigate to **Upload file** and press **Enter**.
6. Type the path to the update file and press **Enter**, for example:

```
./WESPro_RADIO_Production_v40404001_update.bin
```

Note that the update process may take up to three minutes to complete.

7. Use the arrow keys to navigate to **Device reboot** and press **Enter** to reboot the device.

Note

Power cycling the device with the power button is not equivalent to a firmware reboot via the Device reboot option of the CLI tool.

APPENDIX

D

NOTIFICATIONS AND CERTIFICATIONS

This appendix provides notifications and certifications regarding the product described in the guide.

FCC Notifications

Caution

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference and
2. This device must accept any interference received, including interference that may cause undesired operation.

Caution

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RF Exposure Information

The device has been SAR tested and meets SAR requirements. The distance between the user and product antenna should be no less than 0mm.

ISED

This radio transmitter (IC: 29381-1000415A) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 29381-1000415A] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur

Antenna type(s) which can be used with the transmitter:

Table D.1: WES Pro Built-in Antenna

Manufacturer	Antenna Type	Model	Gain (dBi)	Impedance (Ω)
Pasternack	Rubber duck, omnidirectional	PE51RD1021	2.6	50

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF Exposure Requirements

The device has been SAR tested and meets SAR requirements. The distance between the user and product antenna should be no less than 0mm.

L'appareil a été testé en termes de SAR et répond aux normes SAR. La distance entre l'utilisateur et l'antenne du produit ne doit pas être inférieure à 0 mm.

Certifications

The WES Pro is in the process of certification for functional safety by Exida corporation.

APPENDIX

E

WARRANTY

You can view the End-User Agreement on the FORT Robotics website.

You can view the OEM Supply and License Agreement on the FORT Robotics website.

We provide non-safety critical firmware updates to customers whose device has an active Guardian subscription. Guardian allows you to get firmware and software updates, extended support, and warranty coverage beyond the limited one-year hardware warranty term. Guardian is no longer offered so what is our end-user agreement now?